

Integration guide for QVR Surveillance and VCA AI Bridge



Overview

This guide explains how to set up VCA AI Bridge and connect it with QVR Surveillance. By following these steps, you can use VCA AI Bridge for visual analytics and report results to QVR Surveillance. For feature details, refer to the product guide.

How QVR + VCA AI Bridge can help

Imagine a surveillance solution that truly simplifies your daily operations by empowering you to focus on what matters most. By integrating QVR Surveillance with the VCA AI Bridge, you gain a more efficient way to monitor your environment and respond to real incidents with less effort.

- **Confident Compliance:** Easily provide convincing evidence during audits of worker regulations through automatically performed video analytics.
- **Actionable Insights:** Create performance reports rooted in real incidents, helping you make informed decisions and demonstrate continuous improvement.
- **Automatic Violation Detection:** Catch traffic law violations or unauthorized activities without constantly monitoring screens. Let the system alert you to what truly needs attention.
- **Reduced False Alarms:** Rely on advanced analytics to filter out false positives, ensuring you're only notified about events that require real action.
- **Comprehensive Evidence:** Keep video clip evidence for every alert, offering a richer, more reliable record than static snapshots alone.
- **Cost-Efficient and Private:** Avoid the risks, complexities, and costs of cloud services while keeping your data secure, compliant with regulatory requirements, and safer to manage.
- **Effortless Search:** Locate past events quickly with long-term storage and powerful search capabilities—finding evidence has never been easier.
- **Off-Site Backup:** Even if a datacenter is damaged, automatic backups across different sites help preserve these recordings.

With QVR handling surveillance and VCA providing intelligent analytics, you can enjoy peace of mind, improved efficiency, and a simpler, smarter approach to security and compliance.

Revision History

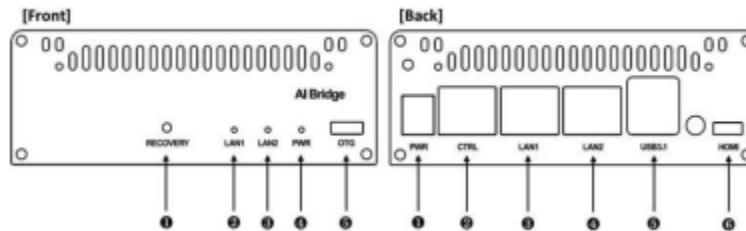
Version	Change log
2026/7/2	Optimized figure placement and layout to improve document compactness.
2026/6/29	Initial version

Table of Contents

Overview	0
How QVR + VCA AI Bridge can help.....	0
Revision History.....	1
Step 1, AI Bridge Installation.....	3
[Front]	3
[Back]	3
Step 2, AI Bridge Network Configuration	4
Step 3, Switching from DHCP to a Static IP Address	4
Step 4, Setting up VCA server.....	4
Step 5, Adding Video Sources	5
A. Add a File as a Video Source	6
B. Add RTSP as a Video Source	7
C. Supported Video Sources	9
Step 6, Configure a Channel	9
A. Add a Zone	9
B. Select a Tracker	12
C. Configure the Rules	15
Setup QVR services	18
Getting Started with NAS	18
Prerequisites	18
Getting Started with QVP Series	18
Prerequisites	18
Getting Started with TVR Series	18
Prerequisites	18
Steps	18
Method 1: Adding VCA AI Bridge to camera list and use built-in event rules	18
Method 2: Adding Customized Events by Event URL	20
Search result from Metadata Search & Event Search	23
Reference.....	25
Appendix 1	25
Appendix 2	25

Initial Setup of AI Bridge

Step 1, AI Bridge Installation



(i) AI Bridge Exterior Overview

[Front]

- ❶ RECOVERY: Press the button quickly 4 times to reboot the system and perform a factory reset.
- ❷ LAN1 status LED: The green LED blinks when the LAN1 port is connected to a network.
- ❸ LAN2 status LED: The green LED blinks when the LAN2 port is connected to a network.
- ❹ Power status LED: The green LED indicates whether the device is powered on.
- ❺ OTG: Technical support purpose.

[Back]

- ❶ PWR: DC12V power connector.
- ❷ CTRL: Technical support purpose.
- ❸ LAN1: 1st RJ45 LAN connector for 1 Gigabit Ethernet.
- ❹ LAN2: 2nd RJ45 LAN connector for 1 Gigabit Ethernet.
- ❺ USB 3.1: Two USB-A connectors for USB devices.
- ❻ HDMI: Micro-HDMI connector for a monitor output.

Step 2, AI Bridge Network Configuration

The default IP address of the device is automatically assigned by a DHCP server when the device is connected to a network. If a DHCP IP cannot be assigned, the device will automatically configure itself with a link-local address. (A link-local address takes the form of 169.254.x.x.) Once the DHCP server becomes available on the network again, the ABP device will automatically obtain and apply a DHCP-assigned IP address. (For more details, please refer to "IP Assignment with No-DHCP Environments" at the link below.)

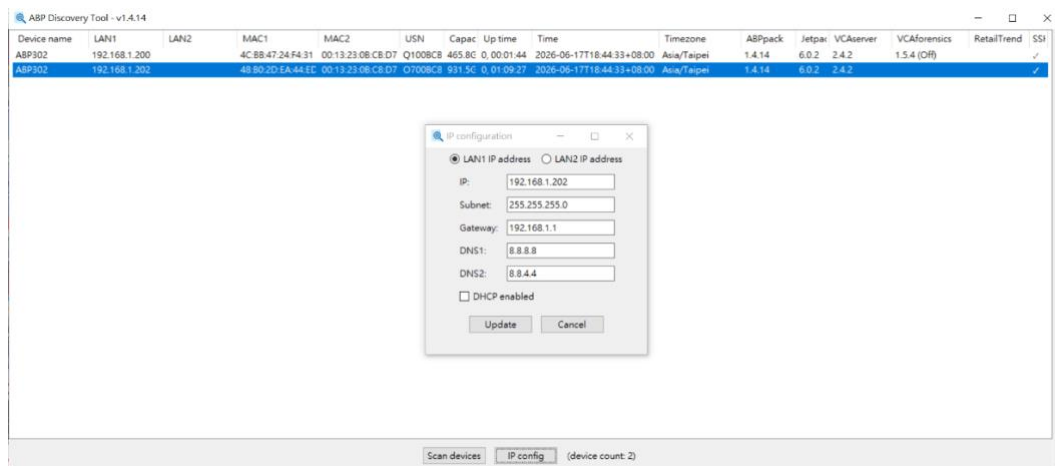
<https://drive.google.com/file/d/1DunHt-SzYpPimrlqW2QgY2owaNPtGmPU/view?usp=sharing>

To discover and change the IP address of devices on the network, use the ABP discovery tool, which is available for download from the link below. The utility runs on Windows 10 and 11. Please prepare a Windows PC if you plan to use this tool for initial configuration.

<https://drive.google.com/drive/folders/1yyHd3YqVAbwDdE2UoSXhZdFzSBtSsQse>

Step 3, Switching from DHCP to a Static IP Address

1. Initiate the discovery of the target device by clicking the "Scan Devices" button in the ABP discovery tool.
2. Open the IP configuration dialog box by selecting the discovered device and clicking the "IP Configuration" button or simply double-clicking the device.
3. To set a static IP address, uncheck the "DHCP Enabled" option within the IP configuration dialog.
4. Confirm your changes by entering the desired static IP address and clicking the "Update" button.



(ii) ABP Discovery Tool

Step 4, Setting up VCA server

1. Power on the device and then open a web browser.

2. Enter the device's IP address followed by port 8080 to access the VCA server.

For example:

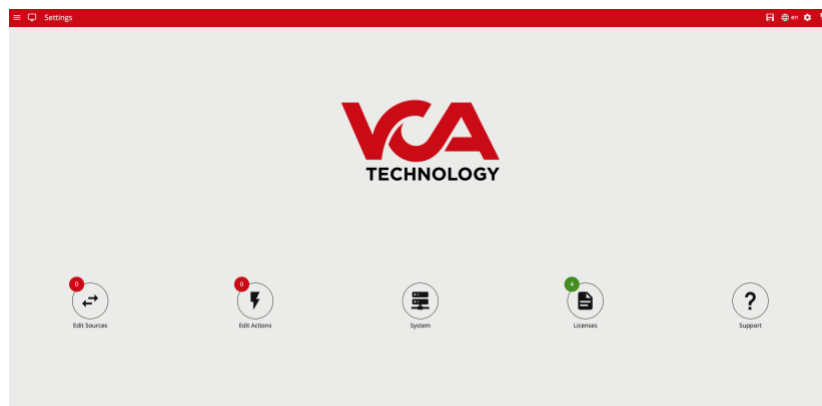
- <http://192.168.10.10:8080> for VCA server

3. On the login page, enter username and password.

- VCA server: admin / admin

4. After entering your credentials, click the "OK" button to proceed.

Notes: Chrome-based browsers are recommended. Some antivirus software may mistakenly block the webpage from being displayed properly; please add the server to the allowed list.



(iii) VCA server software Web UI

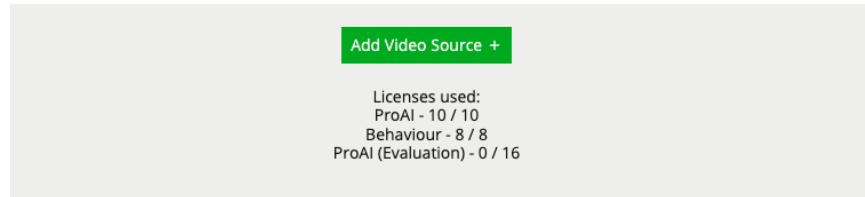
Step 5, Adding Video Sources

To add video sources, please go to Settings → Edit Sources.



Video sources are automatically linked with a channel when added. A preview is provided of the video source showing snapshots of the video content or any warnings. The number of video sources which can be added to the system depends on the user's license. A list of the currently available license types (e.g. ProAI) and the number of those licenses used is provided (e.g. 2 / 12).

License selection allows for a specific license type to be associated with a channel. Licenses can be changed on a video source at any time. However, once a channel is configured with rules and functions linked to a particular license type, **changing the license type for that channel at runtime is not advised.**



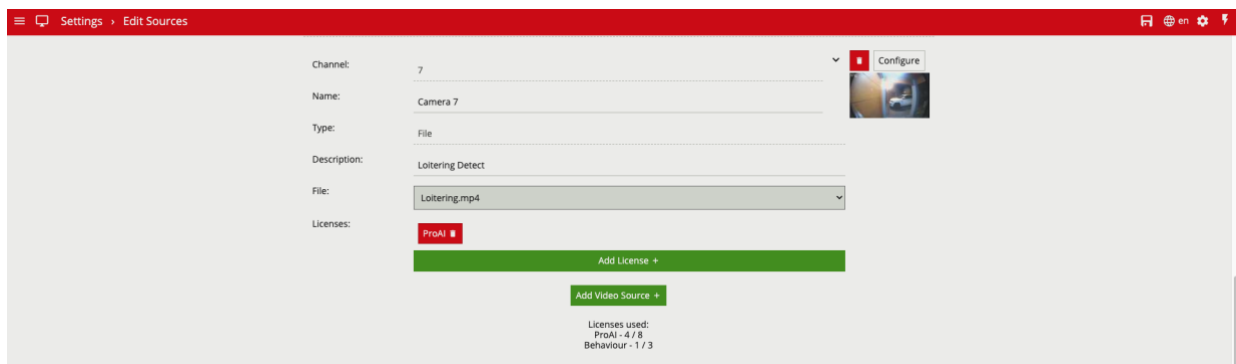
A. Add a File as a Video Source

File sources enable the streaming of video from a file located in a test-clips folder on the host machine. This is useful for demo or benchmark purposes. The folder is in a subdirectory of the default data location:

Use SSH (SCP) to log in to the AI Server and place the files in /var/opt/VCA-Core/test-clips/. The default SSH account and password is vcacore / vcacore, and the system will prompt you to set up a new password to replace the default one. If the password is forgotten, press the reset button four times to restore the settings.

Any video files located in this folder will be listed in the File drop-down menu.

****Please note that when files are added to this folder, the web interface will need to be refreshed for the UI to update the file list in the drop-down menu.****



Properties:

- **Channel:** The channel ID for this video source.
- **File:** The name of the file.

- **Description:** Custom field, the users can input as the remarks, such as the intersection name, floor info, or other relevant information.
- **Configure:** Button to link directly to this source's **channel**.
- **Preview:** snapshot preview of the channel.
- **License:** List of available license types.

B. Add RTSP as a Video Source

The RTSP source streams video from remote RTSP and RTSPS servers such as IP cameras and encoders. The minimum frame rate required for good-quality tracking is 15 fps. The suggested resolution for these RTSP streams is 480p or greater.

The Discover Sources tool can be used to detect and add RTSP sources from ONVIF-compliant devices, such as IP cameras and encoders, or other instances of VCA server with ONVIF enabled.

Note: By design, the VCA AI Server is optimized to run fast and accurately at low resolution, so there is no need to feed it a high-resolution stream. In many scenarios, greater resolution does not improve tracking accuracy and only adds CPU load and slows the system's response time. Use the file-based method described earlier (Add a File as a Video Source) to benchmark detection performance across different resolutions.

Properties:

- **Channel:** The channel ID for this video source.
- **Configure:** Button to link directly to this source's **channel**.
- **Description:** Custom field, the users can input as the remarks, such as the intersection name, floor info, or other relevant information.
- **Preview:** snapshot preview of the channel.
- **URI:** The fully qualified URI to the remote RTSP endpoint.
- **User ID:** The username to access the RTSP endpoint (if applicable).
- **Password:** The password to access the RTSP endpoint (if applicable).

- **Enable Keep-alive:** Periodically sends commands to the RTSP source to keep the RTSP connection alive without interruptions. Most RTSP sources require this option to be enabled. Disable this option only if the RTSP source does not support this behavior.
- **Use RTP over TCP:** Force the RTP stream to be streamed via TCP (instead of UDP). Wherever possible, RTSP streams should be delivered over TCP and not UDP. This is because UDP transport is not robust against packet loss, and dropped packets cause corrupt video, which may cause VCA server to generate false positives.
- **Sync timestamps with RTCP Sender Report:** Sets any timestamp, either within this channel's metadata or RTSP stream out of VCA server, to use the timestamp data attached to the input RTSP source as opposed to the host system time.
- **License:** List of available license types.

When using an RTSPS URI, e.g. `rtsp://192.168.0.25:8554/channels/0`, additional TLS Validation option properties are provided.

- **Enable Trusted Authority:** Checks the SSL certificate used with the RTSPS stream to have come from a trusted authority. Self-signed certificates will not work with this option enabled.
- **Enable Valid Identity:** Checks the source of RTSPS stream matches the Common Name property of the SSL certificate.
- **Enable Certificate Activated:** Checks the start time of the SSL certificate used with the RTSPS stream is in the past.
- **Enable Certificate Not Revoked:** Checks the SSL certificate used with the RTSPS stream has not been revoked by the certificate authority.
- **Enable Certificate Not Expired:** Checks the end time of the SSL certificate used with the RTSPS stream is in the future.

- **Enable Secure Algorithm:** Checks the SSL certificate used with the RTSPS stream is using secure encryption.
- **Enable No Generic Error:** Checks the SSL certificate used with the RTSPS stream is not generating any generic errors.

C. Supported Video Sources

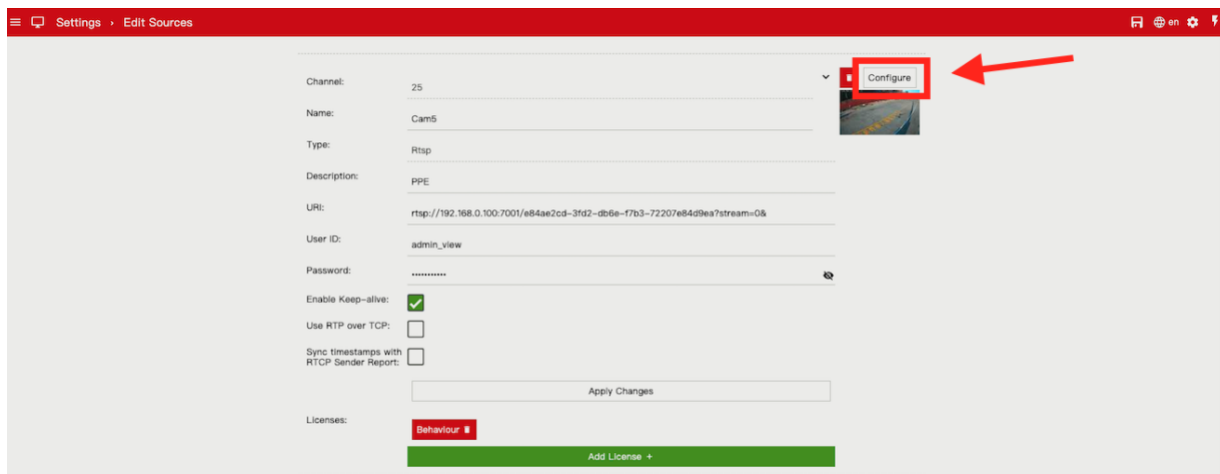
The video codecs supported by VCA server are H.264, H.265, and MPEG4.

Note: Following H.264 profiles can be decoded using hardware acceleration: Constrained Baseline, Main, High, Multiview High and Stereo High

When using an RTSP stream as a source, please ensure it is encoded with one of the supported compression formats. Likewise, when using a file as a source, please note that VCA server is compatible with many video file containers (.mp4, .avi, etc.) but the video file itself must be encoded with one of the above supported compression formats.

Step 6, Configure a Channel

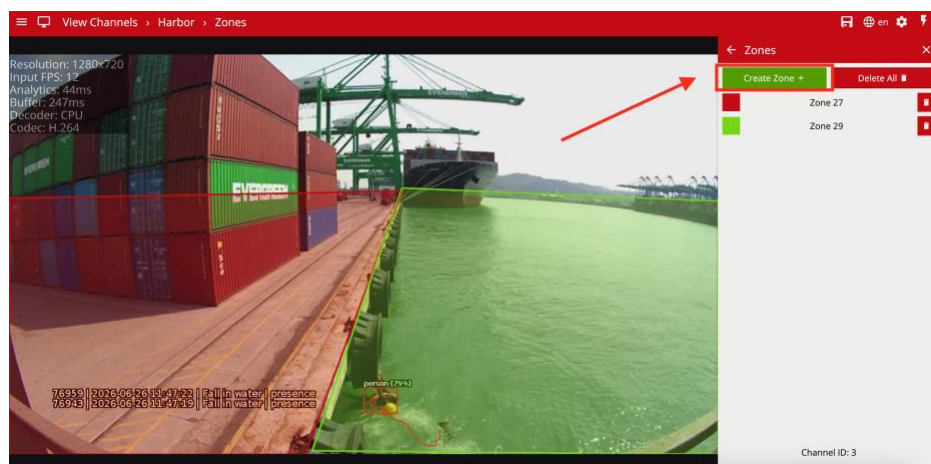
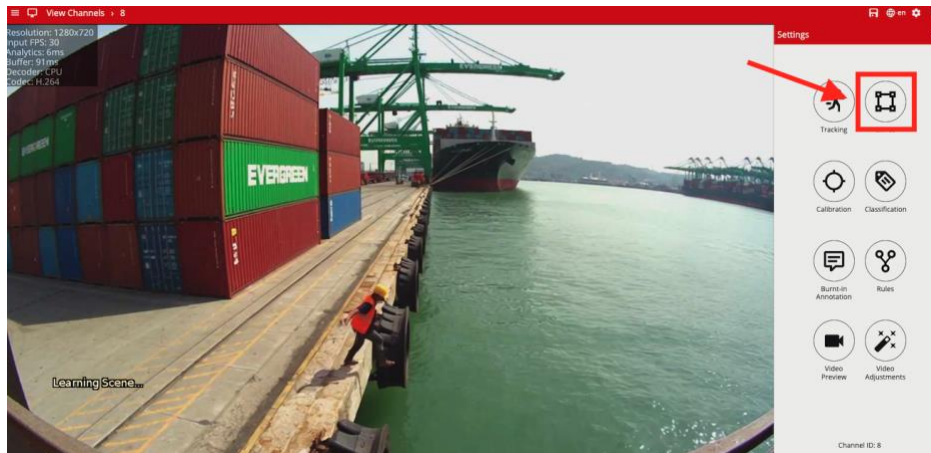
Please click “Configure” to set up the zones, AI engines, and rules.



A. Add a Zone

Zones are the detection areas on which VCA server rules operate. To detect a specific behaviour, a zone must be configured to specify the area where a rule applies.

Zones can be added by clicking the “**Create Zone**” button in the zone settings menu.

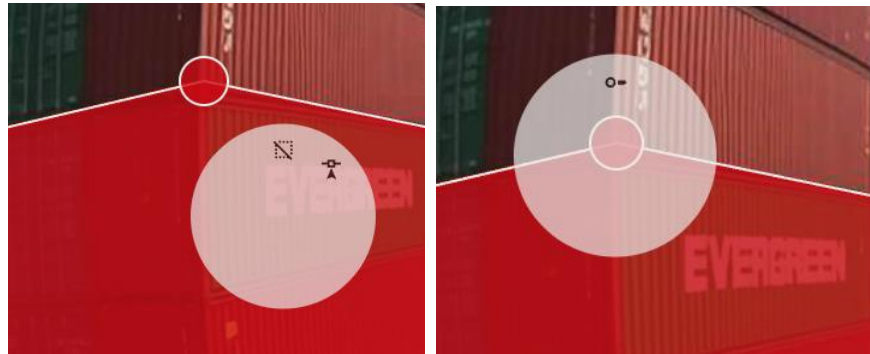


A.1 The Context Menu

Right-clicking or tap-holding (on mobile devices) displays a context menu which contains commands specific to the current context.

The possible actions from the context menu are:

-  Adds a new zone.
-  Deletes an existing zone.
-  Adds a node to a zone.
-  Deletes an existing node from a zone.



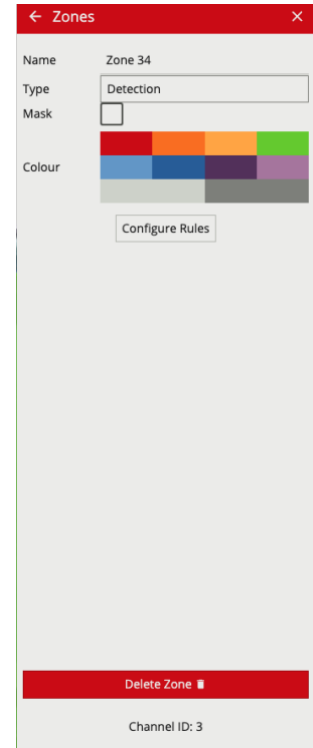
A.2 Positioning Zones

To change the position of a zone, click and drag the zone to a new position. To change the shape of a zone, drag the nodes to create the required shape. New nodes can be added by double-clicking on the edge of the zone or clicking the add node icon  from the context menu.

A.3 Zone Specific Settings

The zone configuration menu contains a range of zone-specific configuration parameters:

- **Name:** The name of the zone, which appears in event notifications.
- **Type:** The type of the zone. Can be one of:
 - **Detection:** A zone which detects tracked objects and to which rules can be applied.
 - **Non-detection:** A zone which specifies an area that should be excluded from VCA server analysis. Objects are not detected in non-detection zones. Useful for excluding areas of potential nuisance alarms from a scene (e.g. waving trees, flashing lights, etc.).
- **Mask:** Click to enable the mask feature for a selected zone.
- **Shape:** The shape of the zone. Can be one of:
 - **Polygon:** A polygonal detection area with at least three nodes. Rules apply to the whole area.
 - **Line:** A single- or multi-segment line with at least two nodes. Rules apply to the length of the line.
- **Colour:** The colour of the zone.
- **Configure Rules:** A shortcut button to navigate directly to the **rules** configuration page.



A.4 Deleting a Zone

Zones can be deleted in the following ways:

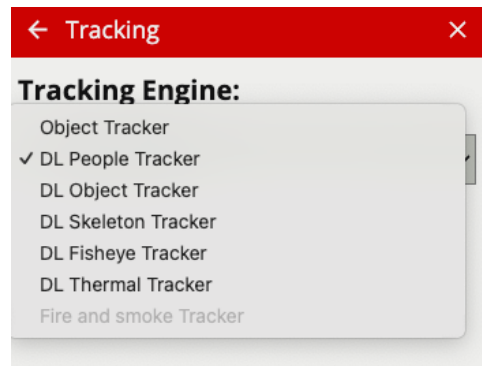
- Select the zone and click the **Delete Zone** button from the zone settings menu.
- Select the zone, display the context menu and select the delete zone icon

B. Select a Tracker



VCA server supports multiple tracker technologies for configured video channels. The available trackers are listed below:

- Object Tracker
- Deep Learning People Tracker (DLPT)
- Deep Learning Skeleton Tracker (DLST)
- Deep Learning Object Tracker (DLOT)
- Deep Learning Thermal Tracker (DLTT)
- Deep Learning Fisheye Tracker (DLFT)
- Hand Object Interaction (HOI) Tracker
- Fire & Smoke Tracker



Under the Trackers menu item is a drop-down menu option for Tracking Engine, under which one of the available trackers can be selected.

Universal Settings

Some settings are universal across all trackers; these are outlined below:

B.1 Loss Of Signal Emit Interval

The Loss Of Signal Emit Interval defines the amount of time between emissions when a channel loses signal to its source.

The default setting is 1 second.

A screenshot of the "Loss Of Signal Emit Interval" settings panel. It features a title bar at the top. Below the title, there is a label "Time:" followed by a text input field containing the number "1", and then the word "Seconds".

B.2 Tamper Detection

The Tamper Detection module is intended to detect camera tampering events such as bagging, de-focusing and moving the camera. This is achieved by detecting large persistent changes in the image.

A screenshot of the "Tamper Detection" settings panel. It has a title bar. Below the title, there are several settings: "Enabled:" with a checked checkbox, "Duration:" with a text input field containing "10" followed by "Seconds", "Area Threshold:" with a text input field containing "20" followed by "%", and "Suppress Alarm on Lights on/off:" with an unchecked checkbox. At the bottom, there is a descriptive note: "Suppress false alarms caused by major light changes. Enabling can reduce sensitivity to genuine alarms."

B.2.1 Enabling Tamper Detection

To enable tamper detection, click the **Enabled** checkbox.

B.2.2 Advanced Tamper Detection Settings

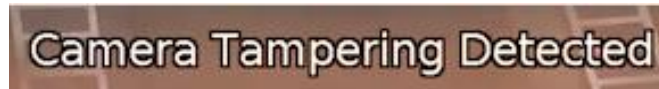
In the advanced tamper detection settings, it is possible to change the thresholds for the area of the image which must be changed and the length of time it must be changed for before the tamper event is triggered.

- **Duration:** the length of time that the image must be persistently changed before the alarm is triggered.
- **Area Threshold:** the percentage area of the image which must be changed for tampering to be triggered.
- **Suppress Alarm on Lights on/off:** Large fast changes to the image lighting, such as switching on/off indoor lighting can cause false tamper events. Enable this option if this is likely to be a problem in the area where the camera is installed. However, this option will reduce sensitivity to genuine alarms, so it is not recommended if rapid light changes are not likely to be a problem.

If false alarms are a problem, the duration and/or area should be increased, so that large transient changes such as close objects temporarily obscuring the camera do not cause false alarms.

B.2.3 Notification

When a tamper event is detected, a tamper event is generated. This event is transmitted through any output elements as well as being displayed in the video stream:



For more information about **Trackers**, please refer to the link below to the “**Tracker**” Chapter of the User Manual.

<https://documentation.vcatechnology.com/#trackers>

C. Configure the Rules



VCA server's rules are used to detect specific events in a video stream. There are three rule types which can be utilised to detect events and trigger actions:

- **Basic Inputs / Rule:** An algorithm that will trigger when a particular behaviour or event has been observed. E.g. Presence. Basic inputs can be used to trigger an action.
- **Filters:** A filter will trigger if the object which has triggered the input rule meets the filter requirements. E.g. is moving at a specific speed. Filters can be used to trigger an action.
- **Conditional Rule:** A logical link between one or more inputs to allow the detection of more complex behaviours. E.g. AND. Conditional rules can be used to trigger an action.

Within VCA server, rule configurations can be as simple as individual **basic inputs** attached to a zone used to trigger an action. Alternatively, rules can be combined into more complex logical rule configurations using **conditional rules** and **filters**. The overarching goal of the rules in VCA server is to help eliminate erroneous alerts being generated, by providing functions to prevent unwanted behaviour from triggering an action.

More detail on the differences between these concepts is outlined below:

C.1 Basic Inputs

A basic input or rule can *only* be used to trigger an action or as an input to another rule type. Basic inputs always require a zone, and potentially some additional parameters. A basic input can be used on its own to trigger an action, although they are often used as an input to other filters or conditional rules.

The complete list of basic inputs is:

- Abandoned
- Absence
- Appear
- Direction

- Directional Crossing
- Disappear
- Dwell
- Enter
- Exit
- Fall
- Fight
- Hands Up
- Occupancy
- Presence
- Stopped
- Tailgating
- Unattended

C.2 Filters

A filter cannot trigger an action on its own as it **requires** another basic input, filter or conditional rule to trigger. An example of this is the Object rule.

The complete list of filters is:

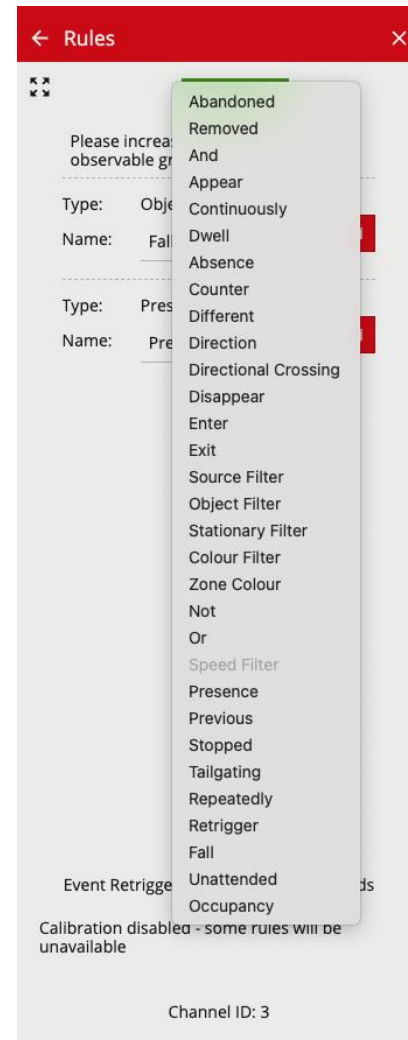
- Accessory Filter
- Colour Filter
- Object Filter
- Other Source Filter
- Retrigger Filter
- Speed Filter
- Zone Colour Filter

C.3 Conditional Rules

A conditional input, like a filter, is one that cannot trigger an action on its own. It **requires** the input of another basic input, conditional rule or filter to be meaningful. An example of this is the AND rule. The AND rule requires two inputs to compare in order to function.

The complete list of conditional rules is:

- And
- Continuously
- Counter
- Not
- Or



- Previous
- Repeatedly

For more information about **Rules**, please refer to the link below to the “**Rules**” Chapter of the User Manual.

<https://documentation.vcatechnology.com/#rules>

Setup QVR services

Getting Started with NAS

QVR Surveillance 3.0 is available through the App Center on each NAS device. The minimum system requirement is QTS or QuTS hero 5.2.x; however, QTS is recommended if the NAS will be dedicated solely to surveillance tasks. If the NAS is used for multiple functions, the maximum number of manageable cameras may decrease, as CPU and disk resources are allocated to other tasks.

Prerequisites

- The NAS should be initialized with appropriate volume and storage pool configurations.
- QVR Surveillance must be installed from the App Center or manually.
- QVR Surveillance should have configured storage space and possess sufficient licenses to manage the intended number of cameras.

Getting Started with QVP Series

The QVP series utilizes QNAP NAS hardware running a customized version of QTS featuring an integrated QVR server. Default disk configurations are optimized for surveillance workloads.

Prerequisites

- The QVP supports VCA AI Bridge starting from firmware version 2.7.
- Storage space should be set up, the system should be ready to add cameras, and sufficient licenses must be available to manage them.

Getting Started with TVR Series

The TVR series operates on a lightweight, purpose-built operating system designed to maximize hardware efficiency for surveillance applications. All features are license-free, eliminating the need for activation processes.

Prerequisites

- Initialize the TVR device.
- Ensure the device has available capacity to manage additional cameras through VCA AI Bridge.

Steps

Although NAS, QVP, and TVR are different platforms, the software features will be similar after the prerequisites are completed.

Method 1: Adding VCA AI Bridge to camera list and use built-in event rules

1. Open “Camera Settings” and select “Add.”

- The QVR servers will scan the local networks to detect cameras on the same LAN. If properly configured, AI Bridge will be listed. If the VCA server does not appear or is not in the same LAN, its IP address can be entered manually.

Add Camera

Camera Selection

The following table lists the cameras found in this NAS network. Select the camera(s) and click Next, or use the advanced search feature to find cameras on other networks. You can also use the filter feature to only display cameras of a specific brand and model. If the camera you want to add is not on the list, click Next to manually add the camera.

Cameras	Brand	Model	IP Address	MAC Address
☒	VCA	VCA Server (CH00)	10.20.70.97	3c:6d:66:03:a8:ab
☐	QNAP	QNAP QUSBCam2 (ch1)	10.20.70.25	24:5e:be:89:e3:bd
☐	QNAP	QNAP QUSBCam2 (ch1)	10.20.71.42	24:5e:be:28:d6:86
☐	ONVIF	ONVIF S+T Cameras (No config)	10.20.70.47	90:09:d0:6a:d0:fc
☐	ONVIF	ONVIF S+T Cameras (No config)	10.20.70.57	00:11:32:a9:ea:ce
☐	QNAP	QNAP QUSBCam2 (ch1)	10.20.70.60	24:5e:be:7e:7f:0f
☐	QNAP	QNAP VirtualCam	10.20.70.61	24:5e:be:7c:19:da

Cameras selected: 1, Cameras that can be selected: 4

Scanning 56% Stop

Cancel Step 1/4 Next

- Select the VCA AI Bridge, press “Next,” and complete the required fields. A VCA AI Bridge supports multiple channels. Ensure the appropriate channel is selected under “Models.”

Edit

Connection Camera Stream

You can edit the camera connection settings.

Preview	Name	Brand Model	IP Address
 Channel 5	Camera 005	VCA VCA Server (CH01)	10.20.70.97

Video Sources

Channel: 1

Name: VCA-LPR

Configure

Channel: 2

Name: test

Configure

4. Press “Test” to confirm the configuration is correct, then finish the setup.

Adding Integrated Events

QVR Surveillance includes pre-defined events compatible with the VCA AI Bridge. Navigate to "Event Rules," and select "Add" to create events. In the "if" field, click "Add" and choose one or more detected event triggers.

The left screenshot shows the 'Add' dialog with the following sections:

- Add Events and Actions:** A section with a description and a table for adding events. The table has columns: Name, Type, Add, Source App, and Operation.
- Trigger criteria:** A section with radio buttons for 'Any event' (selected) and 'All Events: occurring within 10 second(s)'. There is an 'Edit' button next to the 'All Events' option.

The right screenshot shows the 'Add Event' dialog with the following fields and sections:

- Name:** A text input field.
- Type:** A dropdown menu with '2-Wheeled Vehicle Detection' selected.
- Source:** A section with a 'Preview Selected' button and a list of available sources. The list includes '674073QVRDemo1' and '5. Camera 005'.

Ensure that the event is correctly configured in the AI Bridge; otherwise, QVR will not receive the trigger. Appendix 1 provides a list of built-in event types.

Method 2: Adding Customized Events by Event URL

Use this method when VCA AI Bridge detection rules do not map directly to QVR’s built-in Integrated Events, such as repeated actions or customized rule combinations. Instead of adding the VCA server as a camera, QVR treats the AI Bridge as an external detector.

- **Immediate alerts:** Use Event URL to send detection triggers from VCA AI Bridge to QVR Surveillance.
- **Detailed descriptions:** Use External Metadata Labeling to attach additional detection information for search and review.
- **Camera setup:** This method does not require adding the VCA server as a camera in QVR.
- **Screenshot behavior:** By default, Event URL triggers do not generate screenshots. To capture a representative image, pair the event with a recording action from the assigned camera.

Create entry point in Event Rules

When adding events, select the “Event URL” option. Enter an event source name for identification; it will appear in event logs and on the QVR Client for real-time notifications.

×

Add Event

Type an event name, select an event type, and then select an event source. Only the available sources are displayed.

Name:

Event

Events List

Type:

Event URL

An event URL is generated for each event source. You can use the event URL with a third-party interface to trigger QVR Surveillance. To easily differentiate events, use a unique source name for each event.

Event source name:

VCA OtherEvents

Note: To easily differentiate events, use unique source names.

Event URL:

LAN IP

http://192.168.7.174:8080/qvrsurveillance/apis/logical_input.cgi?token=42807

http://10.20.71.82:8080/qvrsurveillance/apis/logical_input.cgi?token=4280753

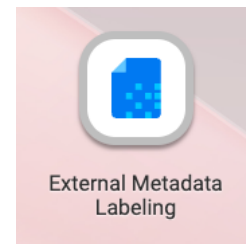
Ok

Cancel

A URL will be generated and can be copied to VCA settings. If the NAS has multiple IPs, several URLs will be created; select one accessible by VCA AI Bridge.

(Optional) Create entry point in External Metadata Labeling

Metadata labeling records extra details about the detection result. It does not create events but serves as a bookmark in QVR Surveillance for future reference.



Open “External Metadata Labeling” in QVR Surveillance and press the “+Add” button at the top-right corner.

 **Add External Event** ×

 Select External Event

 Complete

The metadata of selected external events will be sent to QVR Surveillance. The parameters of external events may vary depending on the types of external event.

External event type: Generic

Transmission method: Metadata URL ⓘ

External event name:

External event description:

CancelApply

 **Add External Event** ×

 Select External Event

 Complete

You have successfully created the following metadata URL.

You can copy and use the metadata URL to enable a third-party device to send its metadata to QVR Surveillance. Metadata can be used to search and play back a recorded video.

LAN IP ☒ Display secure connections

`http://192.168.7.174:8080/qvrsurveillance/qvrip/Event/recvNotify/GENERIC/ID6B41EDCC9267448894320930BAD0`



`http://10.20.71.82:8080/qvrsurveillance/qvrip/Event/recvNotify/GENERIC/ID6B41EDCC9267448894320930BAD06B`



`https://192.168.7.174:443/qvrsurveillance/qvrip/Event/recvNotify/GENERIC/ID6B41EDCC9267448894320930BAD0`



`https://10.20.71.82:443/qvrsurveillance/qvrip/Event/recvNotify/GENERIC/ID6B41EDCC9267448894320930BAD06B`



ⓘ To pair cameras with external events and specify the display format of metadata, click the buttons below. You may configure these settings later.

 Camera Pairing OSD Settings

Finish

Enter the event name and description to identify it. This creates an entry point for use with VCA AI Bridge. “Camera Pairing” lets you select multiple cameras to display extra information in the camera view window.

Input entry point in VCA AI Bridge

Access the VCA AI Bridge dashboard and navigate to the settings menu by pressing the gear button at the top-right corner. Choose “Edit Actions” > Add Action > HTTP

Settings > Edit Actions

Add Action +

Type:	Http	Name:	QVR Meta - Fall down		<
Type:	Http	Name:	QVR Event - Fall down		<
Type:	Http	Name:	QVR Meta - Fight		<
Type:	Http	Name:	QVR Event - Fight		<

Type: Http Name: QVR Event - Fight

URI: http://10.20.71.82/qvrsurveillance/apis/logical_input.cgi?token=514E9265279F4A0B9ABB0231D2C6C816&name=AI-Fight

Select a token to add it to the template string

Port: 8080

Encryption: TLS

Always Trigger: ☐

Sources: [4]: "Fight Sample" - ...

Add Source +

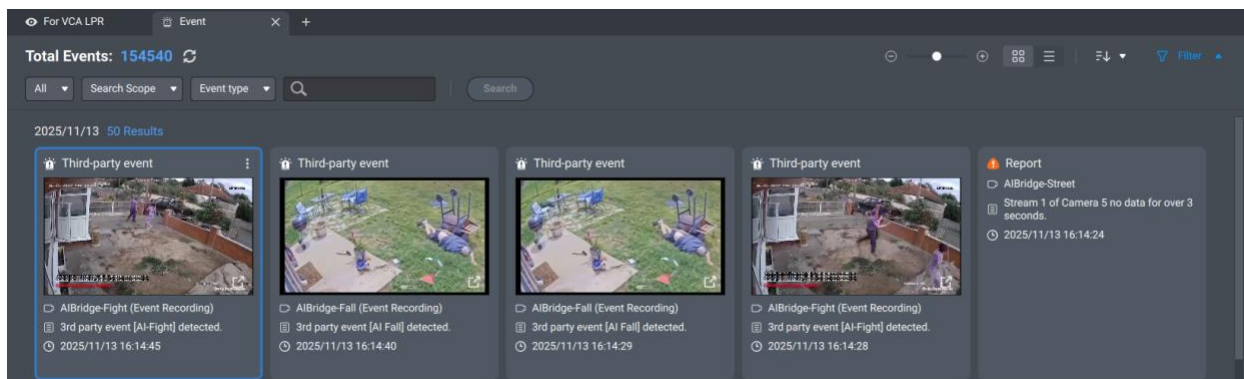
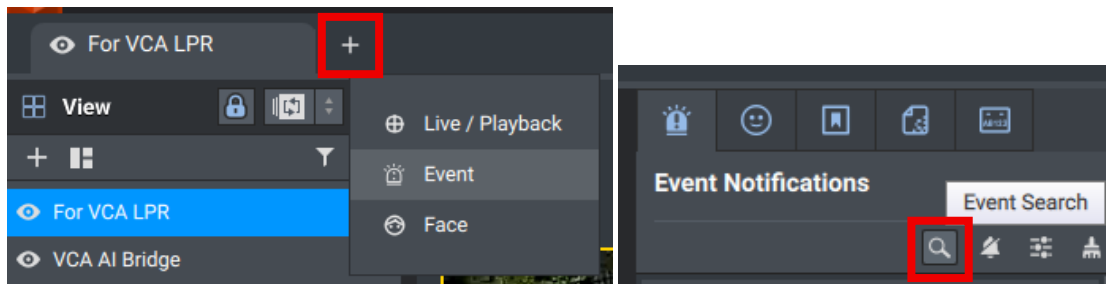
Test

Enter the URL obtained from QVR Surveillance. In the URI field, paste the copied Event URL or Metadata URL. Then scroll to the bottom of the page to select the relevant sources for the rule set within VCA, which will send notifications to QVR Surveillance. The "test" button can be used to confirm that the URI is correct, and it should trigger responses in QVR Surveillance.

When sending information to External Metadata, VCA AI Bridge can include information in the Body and provides a feature to replace variables in the message. A detailed description of `{{tags}}` can be found here: [VCA Documents: Template Tokens](#)

Search result from Metadata Search & Event Search

In QVR Client, events and metadata can be searched by pressing the icons in the notification bar or by adding Event tabs. Events can be searched by keyword and filtered by camera and time.



Reference

Appendix 1

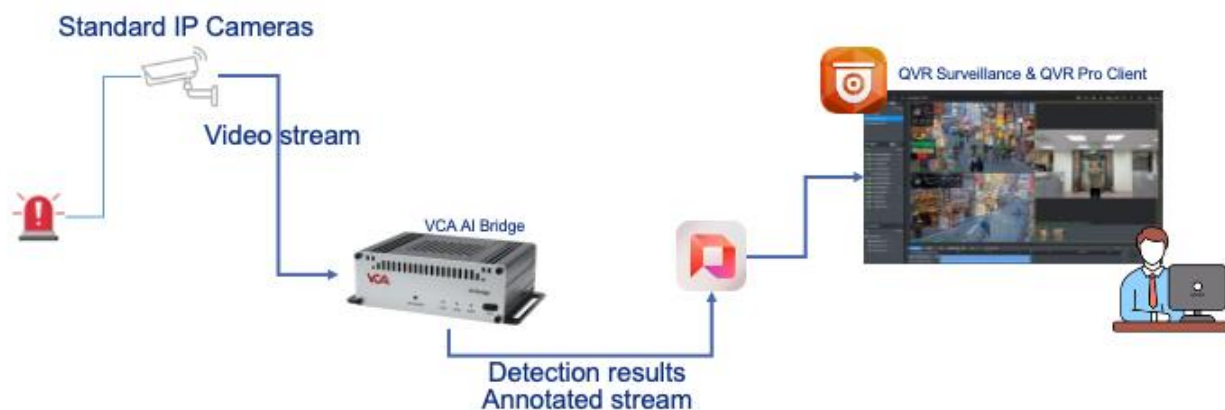
Tables for supported Triggers in QVR server when adding AI Bridge as a Camera, and corresponding detections in VCA AI Bridge

Event Type in QVR server	Detection rule in VCA AI Bridge
Motion Detection	Object Tracker
Cross Line	Presence (Set Zone as Line) Direction
Intrusion Detection	Presence (Set Zone as Polygon Area) Enter
Abandoned Object Detection	Abandoned
Missing Object Detection	Removed
Human Detection	Person
Vehicle Detection	Car, Van, Bus, Truck
Departure Detection	Exit
Loitering Detection	Dwell
2-Wheeled Vehicle Detection	Motor, Bicycle
Event URL	Others not listed above

Appendix 2

Diagrams for linking QVR Surveillance, VCA AI Bridge, and cameras. The diagrams describe data flow rather than actual wiring.

Method 1: Camera connects directly to the AI Bridge, then to QVR Surveillance.



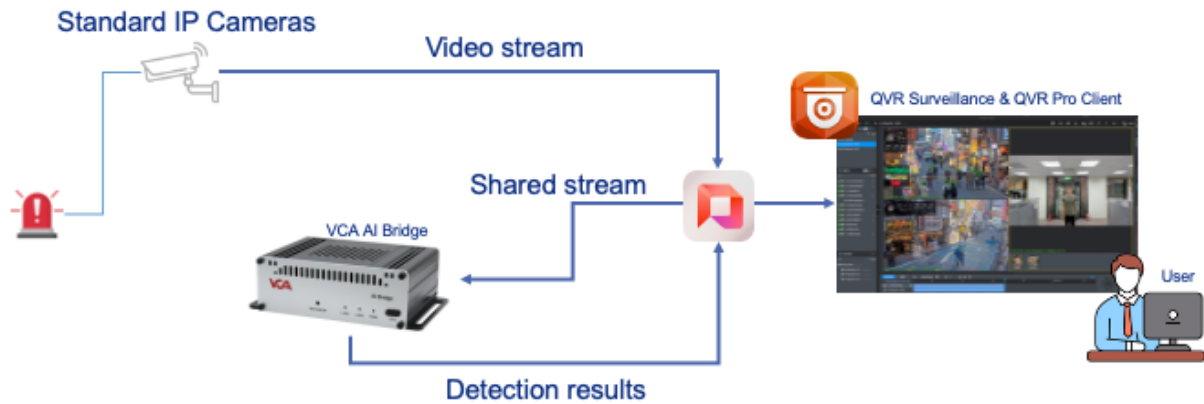
Pros

A more direct way to set up events using predefined types, and annotations can be kept with recordings.

Cons

Only provides one stream for recording.

Method 2:



Pros

QVR records directly from the camera, keeping both main and sub stream recordings.

Cons

The stream to VCA AI Bridge is shared by QVR Surveillance, and annotations will not be recorded. Events must be set up using Event URL (third-party events).